# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051144

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | LIARDET P-Y ET AL: "PREVENTING SPA/DPA IN ECC SYSTEMS USING THE JACOBI FORM" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN : SPRINGER, DE, vol. VOL. 2162, 14 May 2001 (2001-05-14), pages 391-401, XP001061177 ISBN: 3-540-42521-7 | 1,2,12 |
| Y | page 392, line 5 - line 13<br>page 393, line 1 - line 6<br>page 399, line 6 - line 12 | 8-11 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 11 February 2005 | 16. 09. 2005 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Verhoof, P |

Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051144

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | TRICHINA E ET AL: "IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY WITH BUILT-IN COUNTER MEASURES AGAINST SIDE CHANNEL ATTACKS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2002. 4TH INTERNATIONAL WORKSHOP REVISED PAPERS, REDWOOD SHORES, CA, USA, 13-15 AUG. 2002, 13 August 2002 (2002-08-13), pages 98-113, XP001160524 BERLIN, GERMANY, SPRINGER VERLAG | 1,2,12 |
| Y | page 100, line 11 - line 15 * Algorithm 1 * page 105, line 5 - line 10 | 8-11 |
| X | US 2003/079139 A1 (DREXLER HERMANN ET AL) 24 April 2003 (2003-04-24) paragraph [0018] - paragraph [0020] | 1,3-6,12 |
| X | WO 02/088934 A (LIARDET PIERRE-YVAN ; ROMAIN FABRICE (FR); ST MICROELECTRONICS SA (FR)) 7 November 2002 (2002-11-07) page 3, line 1 - line 21; figure 2 | 1,3,4,12 |
| Y | EP 1 296 224 A (HITACHI LTD) 26 March 2003 (2003-03-26) paragraphs [0057], [0058], [0066], [0070] | 8-11 |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2004/051144

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

**see supplemental sheet**

As a result of the prior review under R. 40.2(e) PCT,
no additional fees are to be refunded.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

☒ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

**further information** PCT/ISA/ 210

The International Searching Authority has found that the international application contains multiple (groups of) inventions, as follows:

1. Claims 1, 2 and 7-12

   Secure method for exponentiation in an additive group.

2. Claims 3-6

   Secure method for exponentiation in a multiplicative group.

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/051144

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2003079139 A1 | 24-04-2003 | DE 19963407 A1 | 12-07-2001 |
| | | AU 3015101 A | 09-07-2001 |
| | | CN 1415106 T | 30-04-2003 |
| | | WO 0148706 A1 | 05-07-2001 |
| | | EP 1272984 A1 | 08-01-2003 |
| | | JP 2003525538 T | 26-08-2003 |
| | | ZA 200204746 A | 13-12-2003 |
| WO 02088934 A | 07-11-2002 | FR 2824209 A1 | 31-10-2002 |
| | | EP 1399807 A1 | 24-03-2004 |
| | | WO 02088934 A1 | 07-11-2002 |
| | | JP 2004531762 T | 14-10-2004 |
| | | US 2004179680 A1 | 16-09-2004 |
| EP 1296224 A | 26-03-2003 | JP 2003098962 A | 04-04-2003 |
| | | EP 1296224 A1 | 26-03-2003 |
| | | US 2003059042 A1 | 27-03-2003 |

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/051144

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| X | LIARDET P-Y ET AL: "PREVENTING SPA/DPA IN ECC SYSTEMS USING THE JACOBI FORM" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN : SPRINGER, DE, vol. VOL. 2162, 14 mai 2001 (2001-05-14), pages 391-401, XP001061177 ISBN: 3-540-42521-7 | 1,2,12 |
| Y | page 392, ligne 5 - ligne 13<br>page 393, ligne 1 - ligne 6<br>page 399, ligne 6 - ligne 12 | 8-11 |

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 11 février 2005 | 06 SEPTEMBER 2005<br>06-09-05 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Verhoof, P |

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2004/051144

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| X | TRICHINA E ET AL: "IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY WITH BUILT-IN COUNTER MEASURES AGAINST SIDE CHANNEL ATTACKS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2002. 4TH INTERNATIONAL WORKSHOP REVISED PAPERS, REDWOOD SHORES, CA, USA, 13-15 AUG. 2002, 13 août 2002 (2002-08-13), pages 98-113, XP001160524 BERLIN, GERMANY, SPRINGER VERLAG | 1,2,12 |
| Y | page 100, ligne 11 - ligne 15 * Algorithm 1 * page 105, ligne 5 - ligne 10 | 8-11 |
| X | US 2003/079139 A1 (DREXLER HERMANN ET AL) 24 avril 2003 (2003-04-24) alinéa '0018! - alinéa '0020! | 1,3-6,12 |
| X | WO 02/088934 A (LIARDET PIERRE-YVAN ; ROMAIN FABRICE (FR); ST MICROELECTRONICS SA (FR)) 7 novembre 2002 (2002-11-07) page 3, ligne 1 - ligne 21; figure 2 | 1,3,4,12 |
| Y | EP 1 296 224 A (HITACHI LTD) 26 mars 2003 (2003-03-26) alinéas '0057!, '0058!, '0066!, '0070! | 8-11 |

Demande internationale n°
PCT/EP2004/051144

## RAPPORT DE RECHERCHE INTERNATIONALE

### Cadre II Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 2 de la première feuille)

Conformément à l'article 17.2)a), certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. ☐ Les revendications n°s
se rapportent à un objet à l'égard duquel l'administration n'est pas tenue de procéder à la recherche, à savoir:

2. ☐ Les revendications n°s
se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

3. ☐ Les revendications n°s
sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

### Cadre III Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 3 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

voir feuille supplémentaire

As a result of the prior review under R. 40.2(e) PCT,
no additional fees are to be refunded.

1. ☒ Comme toutes les taxes additionnelles ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. ☐ Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, l'administration n'a sollicité le paiement d'aucune taxe de cette nature.

3. ☐ Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n°s

4. ☐ Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n°s

**Remarque quant à la réserve**

☒ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant.

☐ Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

**SUITE DES RENSEIGNEMENTS INDIQUES SUR PCT/ISA/ 210**

L'administration chargée de la recherche internationale a trouvé plusieurs (groupes d') inventions dans la demande internationale, à savoir:

1. revendications: 1,2,7-12

   Procédé sécurisé de mise à la puissance dans un groupe additive

   ---

2. revendications: 3-6

   Procédé sécurisé de mise à la puissance dans un groupe multiplicative

   ---

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2004/051144

| Document brevet cité au rapport de recherche | Date de publication | Membre(s) de la famille de brevet(s) | Date de publication |
|---|---|---|---|
| US 2003079139 A1 | 24-04-2003 | DE 19963407 A1 | 12-07-2001 |
| | | AU 3015101 A | 09-07-2001 |
| | | CN 1415106 T | 30-04-2003 |
| | | WO 0148706 A1 | 05-07-2001 |
| | | EP 1272984 A1 | 08-01-2003 |
| | | JP 2003525538 T | 26-08-2003 |
| | | ZA 200204746 A | 13-12-2003 |
| WO 02088934 A | 07-11-2002 | FR 2824209 A1 | 31-10-2002 |
| | | EP 1399807 A1 | 24-03-2004 |
| | | WO 02088934 A1 | 07-11-2002 |
| | | JP 2004531762 T | 14-10-2004 |
| | | US 2004179680 A1 | 16-09-2004 |
| EP 1296224 A | 26-03-2003 | JP 2003098962 A | 04-04-2003 |
| | | EP 1296224 A1 | 26-03-2003 |
| | | US 2003059042 A1 | 27-03-2003 |

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

## BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

**IMAGES ARE BEST AVAILABLE COPY.**
**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**